



# 외부 키 관리를 구성합니다

## ONTAP 9

NetApp  
February 12, 2026

# 목차

외부 키 관리를 구성합니다 .....	1
ONTAP 외부 키 관리 구성에 대해 알아보세요 .....	1
ONTAP 클러스터에 SSL 인증서 설치 .....	1
ONTAP 9.6 이상에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화 .....	2
ONTAP 9.5 및 이전 버전에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화 .....	4
ONTAP에서 클러스터된 외부 키 서버를 구성합니다 .....	5
클러스터링된 키 서버를 생성합니다 .....	5
클러스터링된 키 서버를 수정합니다 .....	7
ONTAP 9.6 이상에서 인증 키를 생성합니다 .....	8
ONTAP 9.5 이전 버전에서 인증 키를 만듭니다 .....	10
ONTAP 외부 키 관리를 사용하여 FIPS 드라이브 또는 SED에 데이터 인증 키 할당 .....	12

# 외부 키 관리를 구성합니다

## ONTAP 외부 키 관리 구성에 대해 알아보세요

하나 이상의 외부 키 관리 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다.

온보드 키 관리자를 사용하여 NVE(NetApp Volume Encryption)를 구현할 수 있습니다. ONTAP 9.3 이상에서는 외부 키 관리(KMIP)와 온보드 키 관리자를 사용하여 NVE를 구현할 수 있습니다. ONTAP 9.11.1부터 클러스터에 여러 외부 키 관리자를 구성할 수 있습니다. 을 참조하십시오 [클러스터링된 키 서버를 구성합니다](#).

## ONTAP 클러스터에 SSL 인증서 설치

클러스터와 KMIP 서버는 KMIP SSL 인증서를 사용하여 서로의 ID를 확인하고 SSL 연결을 설정합니다. KMIP 서버와의 SSL 연결을 구성하기 전에, 클러스터에 대한 KMIP 클라이언트 SSL 인증서와 KMIP 서버의 루트 인증 기관(CA)에 대한 SSL 공용 인증서를 설치해야 합니다.

이 작업에 대해

HA 쌍에서는 두 노드가 동일한 퍼블릭 및 프라이빗 KMIP SSL 인증서를 사용해야 합니다. 동일한 KMIP 서버에 여러 HA 쌍을 연결하는 경우, HA 쌍의 모든 노드는 동일한 공용 및 전용 KMIP SSL 인증서를 사용해야 합니다.

시작하기 전에

- 서버에서 시간을 동기화하여 인증서, KMIP 서버 및 클러스터를 생성해야 합니다.
- 클러스터를 위한 공용 SSL KMIP 클라이언트 인증서를 얻어야 합니다.
- 클러스터를 위한 SSL KMIP 클라이언트 인증서와 관련된 개인 키를 얻어야 합니다.
- SSL KMIP 클라이언트 인증서는 암호로 보호되어 있지 않아야 합니다.
- KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 얻어야 합니다.
- MetroCluster 환경에서는 두 클러스터 모두에 동일한 KMIP SSL 인증서를 설치해야 합니다.



클러스터에 인증서를 설치하기 전이나 후에 KMIP 서버에 클라이언트 및 서버 인증서를 설치할 수 있습니다.

단계

1. 클러스터에 SSL KMIP 클라이언트 인증서를 설치합니다.

```
'Security certificate install -vserver admin_svm_name -type client'
```

SSL KMIP 공용 및 개인 인증서를 입력하라는 메시지가 표시됩니다.

```
'cluster1::> security certificate install -vserver cluster1-type client'
```

2. KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 설치합니다.

```
'Security certificate install - vserver admin_svm_name -type server-ca'
```

'cluster1::> security certificate install -vserver cluster1-type server-ca'를 입력합니다

관련 정보

- ["보안 인증서 설치"](#)

## ONTAP 9.6 이상에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

ONTAP 9.11.1부터 기본 키 서버당 최대 3개의 보조 키 서버를 추가하여 클러스터된 키 서버를 생성할 수 있습니다. 자세한 내용은 [을 참조하십시오 클러스터링된 외부 키 서버를 구성합니다](#).

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- MetroCluster 환경에서:
  - 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
  - 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

### 1. 클러스터의 Key Manager 접속 구성:

```
"+ 보안 키 관리자 외부 활성화 - vserver admin_SVM-key-servers host_name | ip_address:port,... -client-cert client_certificate-server-ca-cert server_CA_certificates+
```



- security key-manager external enable 명령이 security key-manager setup 명령을 대체합니다. 명령을 실행하여 외부 키 관리 구성을 변경할 수 security key-manager external modify 있습니다. 에 대한 자세한 내용은 security key-manager external enable ["ONTAP 명령 참조입니다"](#)을 참조하십시오.
- MetroCluster 환경에서 관리 SVM에 대한 외부 키 관리를 구성하는 경우 를 반복해야 합니다 security key-manager external enable 명령을 파트너 클러스터에 표시합니다.

다음 명령을 실행하면 외부 키 서버가 3개인 'cluster1'에 대한 외부 키 관리가 활성화됩니다. 첫 번째 키 서버는 호스트 이름과 포트를 사용하여 지정되고, 두 번째 키는 IP 주소와 기본 포트를 사용하여 지정되며, 세 번째 키는 IPv6 주소와 포트를 사용하여 지정됩니다.

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

'Security key-manager external show-status-node\_name-vserver SVM-key-server host\_name|ip\_address:port-key-server-status available|not-responding|unknown'



`security key-manager external show-status` 명령이 `security key-manager show -status` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external show-status` link:<https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html> ["ONTAP 명령 참조입니다"^]을 참조하십시오.

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
node1			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

6 entries were displayed.

관련 정보

- [클러스터링된 외부 키 서버를 구성합니다](#)
- ["보안 키 관리자 외부 활성화"](#)
- ["보안 키 관리자 외부 상태 표시"](#)

# ONTAP 9.5 및 이전 버전에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

이 작업에 대해

ONTAP는 클러스터의 모든 노드에 대해 KMIP 서버 연결을 구성합니다.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
- MetroCluster 환경에서는 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터 노드에 대한 Key Manager 접속 구성:

보안 키 관리자 설정

키 관리자 설정이 시작됩니다.



MetroCluster 환경에서는 두 클러스터에서 모두 이 명령을 실행해야 합니다. 자세히 알아보세요 [security key-manager setup](#) 에서 "[ONTAP 명령 참조입니다](#)".

2. 각 프롬프트에 적절한 응답을 입력합니다.

3. KMIP 서버 추가:

'Security key-manager add-address key\_management\_server\_ipaddress

```
cluster1::> security key-manager add -address 20.1.1.1
```



MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

4. 이중화를 위해 KMIP 서버를 추가로 추가합니다.

'Security key-manager add-address key\_management\_server\_ipaddress

```
cluster1::> security key-manager add -address 20.1.1.2
```



MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

5. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

보안 키 관리자 표시 상태

이 절차에 설명된 명령에 대해 자세히 알아보세요. ["ONTAP 명령 참조입니다"](#).

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

```
volume encryption conversion start
```

볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다. MetroCluster 환경에서는 외부 키 관리자를 두 사이트에 모두 구성해야 합니다.

## ONTAP에서 클러스터된 외부 키 서버를 구성합니다

ONTAP 9.11.1부터 SVM에서 클러스터링된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 클러스터형 키 서버를 사용하면 SVM에서 기본 키 서버와 보조 키 서버를 지정할 수 있습니다. ONTAP 키를 등록하거나 검색할 때 먼저 기본 키 서버에 액세스를 시도한 후 작업이 성공적으로 완료될 때까지 순차적으로 보조 서버에 액세스를 시도합니다.

NetApp Storage Encryption(NSE), NetApp Volume Encryption(NVE), NetApp Aggregate Encryption(NAE) 키에 외부 키 서버를 사용할 수 있습니다. SVM은 최대 4개의 기본 외부 KMIP 서버를 지원할 수 있습니다. 각 기본 서버는 최대 3개의 보조 키 서버를 지원할 수 있습니다.

이 작업에 대해

- 이 프로세스는 KMIP를 사용하는 주요 서버만 지원합니다. 지원되는 키 서버 목록을 보려면 ["NetApp 상호 운용성 매트릭스 툴"](#)을 확인하십시오.

시작하기 전에

- ["SVM에 대해 KMIP 키 관리를 활성화해야 합니다"](#).
- 클러스터의 모든 노드에서 ONTAP 9.11.1 이상이 실행되고 있어야 합니다.
- 서버 목록의 순서는 다음과 같습니다. `-secondary-key-servers` 매개변수는 외부 키 관리(KMIP) 서버의 액세스 순서를 반영합니다.

### 클러스터링된 키 서버를 생성합니다

구성 절차는 기본 키 서버를 구성했는지 여부에 따라 달라집니다.

## SVM에 1차 및 2차 키 서버를 추가합니다

### 단계

1. 클러스터(관리 SVM)에 대해 키 관리가 활성화되지 않았는지 확인하세요.

```
security key-manager external show -vserver <svm_name>
```

SVM에 이미 최대 4개의 기본 키 서버가 활성화되어 있는 경우 새 기본 키 서버를 추가하기 전에 기존 기본 키 서버 중 하나를 제거해야 합니다.

2. 기본 키 관리자를 활성화합니다.

```
security key-manager external enable -vserver <svm_name> -key-servers  
<primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs  
<server_ca_cert_names>
```

- 포트를 지정하지 않으면 `-key-servers` 매개변수의 경우 기본 포트 5696이 사용됩니다.



실행 중이라면 `security key-manager external enable MetroCluster` 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

3. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 심표로 구분하여 나열할 수 있습니다.

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.



실행 중이라면 `security key-manager external MetroCluster` 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

## 기존 기본 키 서버에 보조 키 서버를 추가합니다

### 단계

1. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 심표로 구분하여 나열할 수 있습니다.

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.



실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버에 대한 자세한 내용은 다음을 참조하세요. [\[mod-secondary\]](#).

## 클러스터링된 키 서버를 수정합니다

보조 키 서버를 추가 및 제거하고, 보조 키 서버의 액세스 순서를 변경하거나, 특정 키 서버의 지정(기본 또는 보조)을 변경하여 클러스터형 외부 키 서버를 수정할 수 있습니다. MetroCluster 구성에서 클러스터된 외부 키 서버를 수정하는 경우 NetApp 두 클러스터에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버를 수정합니다

``security key-manager external modify-server`` 명령의 ``-secondary-key-servers`` 매개변수를 사용하여 보조 키 서버를 관리합니다. 그만큼 ``-secondary-key-servers`` 매개변수는 심표로 구분된 목록을 허용합니다. 목록에서 보조 키 서버의 지정된 순서는 보조 키 서버의 액세스 순서를 결정합니다. 보조 키 서버가 다른 순서로 입력된 상태에서 ``security key-manager external modify-server`` 명령을 실행하여 액세스 순서를 수정할 수 있습니다. 보조 키 서버에 대한 포트 번호를 포함하지 마세요.



실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

보조 키 서버를 제거하려면 유지하려는 키 서버를 포함하세요. `-secondary-key-servers` 매개변수를 선택하고 제거하려는 매개변수는 생략합니다. 모든 보조 키 서버를 제거하려면 인수를 사용하세요. `-`, 없음을 의미합니다.

기본 및 보조 키 서버를 변환합니다

다음 단계에 따라 특정 키 서버의 지정(기본 또는 보조)을 변경할 수 있습니다.

기본 키 서버를 보조 키 서버로 변환

단계

1. SVM에서 기본 키 서버를 제거합니다.

```
security key-manager external remove-servers
```



실행 중이라면 `security key-manager external remove-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

2. 수행하다 **클러스터링된 키 서버를 생성합니다** 이전 기본 키 서버를 보조 키 서버로 사용하는 절차입니다.

보조 키 서버를 기본 키 서버로 변환

단계

1. 기존 기본 키 서버에서 보조 키 서버를 제거합니다.

```
security key-manager external modify-server -secondary-key-servers
```

- 실행 중이라면 `security key-manager external modify-server -secondary-key-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.
- 기존 키 서버를 제거하는 동안 보조 키 서버를 기본 키 서버로 변환하는 경우, 제거 및 변환을 완료하기 전에 새 키 서버를 추가하려고 하면 키 중복이 발생할 수 있습니다.

1. 수행하다 **클러스터링된 키 서버를 생성합니다** 이전 보조 키 서버를 새로운 클러스터형 키 서버의 기본 키 서버로 사용하는 절차입니다.

참조하다 [\[mod-secondary\]](#) 자세한 내용은.

관련 정보

- 자세히 알아보세요 `security key-manager external` 에서 "[ONTAP 명령 참조입니다](#)"

## ONTAP 9.6 이상에서 인증 키를 생성합니다

'Security key-manager key create' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 것과 동일한 인증 키를 FIPS 규정 준수에 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- Onboard Key Manager가 활성화된 경우 이 명령은 지원되지 않습니다. 그러나 Onboard Key Manager가 활성화되면 두 개의 인증 키가 자동으로 생성됩니다. 키는 다음 명령을 사용하여 볼 수 있습니다.

```
security key-manager key query -key-type NSE-AK
```

- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.
- 사용하여 명령을 수 security key-manager key delete 사용하지 않는 키를 삭제할 있습니다. security key-manager key delete `지정된 키가 현재 ONTAP에서 사용 중인 경우 명령이 실패합니다. (이 명령을 사용하려면 보다 큰 Privileges가 있어야 `admin 합니다.)



MetroCluster 환경에서 키를 삭제하기 전에 키가 파트너 클러스터에서 사용되고 있지 않은지 확인해야 합니다. 파트너 클러스터에서 다음 명령을 사용하여 키가 사용되고 있지 않은지 확인할 수 있습니다.

- storage encryption disk show -data-key-id <key-id>
- storage encryption disk show -fips-key-id <key-id>

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

```
security key-manager key create -key-tag <passphrase_label> -prompt-for -key true|false
```



설정을 prompt-for-key=true 사용하면 클러스터 관리자에게 암호화된 드라이브를 인증할 때 사용할 암호를 묻는 메시지가 표시됩니다. 그렇지 않으면 시스템이 자동으로 32바이트 암호를 생성합니다. security key-manager key create `명령이 `security key-manager create-key 명령을 대체합니다. 에 대한 자세한 내용은 security key-manager key create "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예제에서는 32바이트 암호를 자동으로 생성하는 "cluster1"에 대한 인증 키를 만듭니다.

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 인증 키가 생성되었는지 확인합니다.

```
security key-manager key query -node node
```



`security key-manager key query` 명령이 `security key-manager query key` 명령을 대체합니다.

출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager key query
  Vserver: cluster1
  Key Manager: external
  Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                   NSE-AK    yes
  Key ID: <id_value>
node1                                   NSE-AK    yes
  Key ID: <id_value>

  Vserver: cluster1
  Key Manager: external
  Node: node2

Key Tag                                Key Type  Restored
-----                                -
node2                                   NSE-AK    yes
  Key ID: <id_value>
node2                                   NSE-AK    yes
  Key ID: <id_value>
```

에 대한 자세한 내용은 security key-manager key query "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

관련 정보

- "[저장 암호화 디스크 표시](#)"

## ONTAP 9.5 이전 버전에서 인증 키를 만듭니다

'Security key-manager create-key' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야

합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 FIPS 준수에 동일한 인증 키를 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- 온보드 키 관리가 활성화된 경우 이 명령은 지원되지 않습니다.
- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.

키 관리 서버 소프트웨어를 사용하여 사용하지 않는 키를 삭제한 다음 명령을 다시 실행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

보안 키 관리자 만들기 키

에 대한 자세한 내용은 `security key-manager create-key` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.



출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

다음 예제에서는 "cluster1"에 대한 인증 키를 만듭니다.

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. 인증 키가 생성되었는지 확인합니다.

보안 키 관리자 쿼리

에 대한 자세한 내용은 `security key-manager query` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag      Key Type  Restored
-----
cluster1-01  NSE-AK   yes
      Key ID: <id_value>

      Node: cluster1-02
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag      Key Type  Restored
-----
cluster1-02  NSE-AK   yes
      Key ID: <id_value>
```

## ONTAP 외부 키 관리를 사용하여 FIPS 드라이브 또는 SED에 데이터 인증 키 할당

'스토리지 암호화 디스크 수정' 명령을 사용하여 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당할 수 있습니다. 클러스터 노드는 이 키를 사용하여 드라이브에서 암호화된 데이터를 잠그거나 잠금 해제합니다.

이 작업에 대해

자체 암호화 드라이브는 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 무단 액세스로부터 보호됩니다. 키 ID 0x0이 있는 제조업체 보안 ID(MSID)는 SAS 드라이브의 표준 기본값입니다. NVMe 드라이브의 경우 표준 기본값은 빈 키 ID로 표시되는 null 키입니다. 키 ID를 자체 암호화 드라이브에 할당하면 시스템은 해당 인증 키 ID를 기본값이 아닌 값으로 변경합니다.

이 절차는 중단되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에 데이터 인증 키 할당:

'Storage encryption disk modify -disk\_disk\_ID\_-data-key-id\_key\_ID\_'

에 대한 자세한 내용은 `storage encryption disk modify` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.



'Security key-manager query-key-type NSE-AK' 명령어를 이용하여 키 ID를 확인할 수 있다.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
<id_value>
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

## 2. 인증 키가 할당되었는지 확인합니다.

스토리지 암호화 디스크 표시

에 대한 자세한 내용은 `storage encryption disk show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data <id_value>  
0.0.1     data <id_value>  
[...]
```

### 관련 정보

- "[저장 암호화 디스크 표시](#)"
- "[저장 암호화 디스크 표시 상태](#)"

## 저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.